[COMPANY NAME]
[Add your company logo / letterhead and registered address here]

Physical Security Policy

HOW TO USE THIS TEMPLATE
This template is mostly complete and pre-filled with standard Indian practice. You should not have to fill many blanks.
Text in blue is a default that companies commonly change. Skim the blue text and edit only what differs for you.
Add your company name and letterhead once, in the header above. The body refers to "the Company".
Tailor the access zones, CCTV retention period and visitor rules to your actual premises; if you operate from a shared or co-working space, note which controls are managed by the landlord or building operator and which the Company owns.
Have it reviewed by a qualified HR or legal professional before you adopt it, and delete this box.
Provided by CFOmatrix (cfomatrix.in). General template, not legal advice.

Policy owner	**[Human Resources / IT / Compliance]**
Effective date	**[DD MMM YYYY]**
Version	1.0
Approved by	**[Name, Title]**

1. Purpose

This policy sets out how the Company protects its people, premises, equipment, information and other assets from unauthorised physical access, theft, damage, tampering, interference and environmental harm. Physical security is the foundation of information security: a strong logical control set can be undone by an unlocked server room, an unescorted visitor or an unshredded document. This policy establishes a consistent, defensible baseline of physical and environmental controls across all Company locations.

The policy is designed to support the Company's wider information security objectives and to align with recognised control frameworks, including **ISO/IEC 27001** (Annex A physical and environmental controls) and **SOC 2** (Common Criteria for logical and physical access). It also supports the Company's obligations to safeguard personal data under the Digital Personal Data Protection Act, 2023 (DPDP Act), where that data is held on paper or on physical media and systems on the premises.

2. Scope

This policy applies to:

- All Company premises, including head office, branch offices, data centre or server rooms, network and communications rooms, stores and any leased or co-working space occupied by the Company.

- All employees, directors, interns, trainees, contractors, consultants, vendors, auditors, visitors and any other person who enters Company premises or handles Company physical assets.
- All physical assets, including buildings, server and network equipment, end-user devices, removable media, paper records, access cards, keys and security systems.
- Work-from-home and remote-work locations to the extent set out in Section 12 (remote and hybrid working).

Where the Company occupies shared or third-party-managed premises, this policy applies to the Company's own controls; controls operated by the landlord or building management are governed by the relevant lease or service agreement, and the Company will obtain reasonable assurance that those controls are adequate.

3. Definitions

- Authorised Person: an individual whose access to a given area or asset has been formally approved under this policy.
- Restricted Area: any zone where access is limited to named individuals, for example server rooms, network/communications rooms, finance records storage and HR records storage.
- Visitor: any person who is not an employee or a contractor with standing access, including clients, candidates, auditors, delivery personnel and family members.
- Access Credential: any physical or logical means of entry, including access cards, fobs, PINs, biometric enrolment and physical keys.
- Asset Owner: the role accountable for a specific asset or area and for approving access to it.
- Tailgating: an unauthorised person following an authorised person through a controlled door without presenting their own credential.

4. Security Zones and Access Control

The Company classifies its premises into security zones, each with a defined level of access control. Access is granted on a least-privilege, need-to-enter basis and is reviewed periodically.

Zone	Examples	Who may enter	Control
Public	Reception, visitor waiting area	Anyone, supervised	Reception sign-in, staffed during hours
General work area	Open-plan desks, meeting rooms	Employees and escorted visitors	Access card at entry door
Restricted	Finance and HR records, comms rooms	Named, approved staff only	Card plus access list, logged
High security	Server room, data centre, network core	**Named IT/infra staff only**	Dual control or card plus PIN/biometric, logged, CCTV

Key access rules:

- Entry doors to general work areas and above must be fitted with **electronic access control** (card or fob readers) and must fail to a secure state on power loss where life-safety codes permit, while always allowing free egress.
- Access to Restricted and High Security zones must be individually approved by the relevant Asset Owner and the **IT/Security Manager** before a credential is enabled.
- Doors to Restricted and High Security areas must not be propped open. Where a door is held open for deliveries or maintenance, a named person must remain present until it is secured.
- Tailgating and credential sharing are prohibited. Every person must badge in with their own credential; one badge, one person.
- Master keys and override credentials are held by **the Facilities Manager and the IT/Security Manager** only, stored in a locked key cabinet, and signed in and out.

5. Access Cards, Keys and Credentials

- Access cards and physical keys are Company property, are issued to a named individual, and must not be lent, copied or transferred.
- Access cards are issued by **HR/Facilities** on the employee's joining date after the access-approval workflow is complete, and the level of access is set to the minimum required for the role.
- Lost or stolen cards, fobs or keys must be reported to **security@company.in** or **the Facilities Manager** immediately so the credential can be deactivated. Replacement may attract a fee of **Rs 250** per card at the Company's discretion.
- PINs and biometric data used for access control are confidential, must not be shared, and (where biometrics are used) are processed in line with the Company's data protection obligations under the DPDP Act, with consent, purpose limitation and secure storage.
- On any change of role, access rights are re-evaluated and adjusted within **5 working days**.
- On exit, all cards, keys and credentials are surrendered as part of the offboarding checklist and are deactivated on or before the last working day. Same-day deactivation applies to any termination for cause.
- An access-rights review is performed at least **every 6 months** for Restricted and High Security zones, reconciling the active access list against current staff and roles; orphaned or excessive access is revoked.

6. Visitor Management

- All visitors must enter through **reception**, present valid photo identification, sign the visitor register (or electronic visitor system), and be issued a visibly distinct visitor badge.
- Visitors must be sponsored by a named employee (the host), who is responsible for the visitor's conduct, escort and sign-out.
- Visitors must be escorted at all times in General work areas and above, and must never be left unattended in Restricted or High Security zones. Access by visitors to High Security zones requires prior written approval from the **IT/Security Manager**.

- The visitor register or system must capture: name, organisation, host, purpose, date, time in and time out, and badge number. Records are retained for **12 months** and are treated as confidential.
- Delivery, courier and maintenance personnel are treated as visitors. Deliveries are received at **reception or the loading area** and not within Restricted zones.
- Visitor badges must be returned on exit; unreturned badges are reported to Facilities for deactivation.

7. Server Rooms, Network Areas and Equipment Security

Server rooms, data centres and network/communications rooms hold the Company's most critical and sensitive assets and are designated High Security zones.

- Access is limited to a short, named list of **IT and infrastructure staff**, maintained by the **IT/Security Manager**, and is logged on every entry and exit.
- Third-party engineers and vendors entering these areas must be pre-authorised, escorted by Company IT staff, and recorded in the access log with the work performed.
- Racks and cabinets containing critical equipment must be physically locked; keys are controlled under Section 4.
- Equipment must not be moved, added or removed from these areas without an approved change/asset record.
- Network cabling, patch panels and wireless access points must be installed so that they are not exposed to casual tampering; unused network ports in public and general areas should be disabled or physically secured.
- A current asset register of equipment located in these areas is maintained and reconciled at least **annually**.
- Where the Company uses a third-party or cloud data centre, the Company obtains assurance of the provider's physical security controls (for example a current **SOC 2 Type II** or **ISO 27001** report) at least annually.

8. CCTV and Surveillance

- CCTV is operated at **entry/exit points, reception, server room doors and other sensitive areas** to deter and detect unauthorised access and to support incident investigation.
- CCTV is operated for legitimate security purposes only. It is not used for covert monitoring of employees' routine work, and cameras are not installed in toilets, changing areas, nursing/feeding rooms or other areas with a reasonable expectation of privacy.
- Visible signage notifying that CCTV is in operation is displayed at monitored entrances, supporting transparency and the notice principle under the DPDP Act.
- CCTV footage is personal data where individuals are identifiable; it is processed lawfully, access is restricted to **the Facilities Manager, IT/Security Manager and authorised security staff**, and footage is not shared externally except to law enforcement on lawful request or as required by law.

- Footage is retained for **30 days** and then securely overwritten or deleted, unless retained longer for a specific investigation, legal hold or law-enforcement request.
- Requests by a data principal in relation to their own footage are handled through the Company's data protection grievance process.

9. Clear Desk, Clear Screen and Secure Disposal

- Clear Desk: when a workstation is left unattended for an extended period and at the end of each working day, employees must clear sensitive documents and removable media into locked storage. This policy operates together with the Company's **Clear Desk and Clear Screen Policy** and **Information Security Policy**.
- Clear Screen: screens must be locked when unattended (manual lock plus automatic lock after **10 minutes** of inactivity), and confidential information must not be left displayed where visitors can see it.
- Printing: sensitive documents must be collected promptly; use of secure or pull-printing is encouraged. Documents left at printers are treated as a clear-desk breach.
- Secure Disposal of paper: confidential and personal-data documents must be destroyed using **cross-cut shredders** or locked secure-shredding bins, never placed in ordinary waste. Disposal of bulk records may be outsourced to a certificated destruction vendor, who must provide a certificate of destruction.
- Secure Disposal of media and devices: hard drives, SSDs, USB media, phones and other devices are sanitised by secure wipe or, where wiping is not possible, by physical destruction, before disposal, resale or return. A record of media sanitisation/destruction is maintained. This supports the DPDP Act principle of retention limitation and erasure when personal data is no longer needed.

10. Environmental Controls

The Company protects equipment and records against environmental hazards.

- Power: critical equipment (servers, network, security systems) is protected by **UPS** units sized for safe shutdown, with **a backup generator or DG set** where business needs require, and surge protection. UPS batteries and generators are tested at least **quarterly**.
- Fire: premises are equipped with **smoke detectors, fire alarms and appropriate extinguishers (clean-agent/CO2 for server areas, not water)**; fire exits are kept unobstructed; fire drills are conducted at least **once a year** and detection/suppression systems are serviced per the supplier schedule and local fire-safety regulations.
- Climate: server and network rooms are temperature and humidity controlled with **air conditioning** sized for the load; high-criticality rooms have temperature monitoring with alerting.
- Water and flood: equipment is kept off floor level where flood risk exists, and rooms are checked for leaks; water and beverages are kept away from equipment in server areas.

- Housekeeping: cabling is managed and labelled; combustible materials and clutter are kept out of server rooms; no eating or drinking is permitted in High Security equipment areas.
- Maintenance: building and environmental systems are maintained on a documented schedule, and maintenance visits to Restricted/High Security areas are escorted and logged.

11. Roles and Responsibilities

Role	Responsibility
Management / Director	Owns this policy, approves the security budget, accepts residual risk
IT / Security Manager	Owns access to High Security zones, access reviews, CCTV governance, incident handling
Facilities Manager	Day-to-day premises security, keys, visitor system, environmental controls, maintenance
HR	Triggers card issue/revocation on joining, role change and exit; communicates the policy
Asset Owners	Approve access to their Restricted area or asset, review access lists
Hosts	Supervise and escort their visitors and ensure sign-out
All staff	Badge in individually, prevent tailgating, follow clear-desk rules, report incidents

12. Remote and Hybrid Working

- Employees working from home or other remote locations must keep Company devices and any printed Company information physically secure and out of sight of others, and must lock screens when unattended.
- Confidential and personal-data documents must not be printed at home unless necessary and, if printed, must be securely shredded or returned for destruction.
- Company devices must not be left unattended in vehicles or public places, and must use full-disk encryption and screen-lock as required by the **Information Security Policy**.
- Loss or theft of any Company device or data while remote must be reported to **security@company.in** without delay, in line with Section 14.

13. Compliance, Monitoring and Audit

- Access logs, visitor records and CCTV are reviewed periodically and on the occurrence of any incident.
- Physical security walkthroughs (checking doors, locks, badges, clear desks, server-room access and environmental systems) are conducted at least **quarterly** by **Facilities and IT**, with findings tracked to closure.
- This policy and its controls are subject to internal and external audit, including audits under **ISO 27001 / SOC 2** programmes where applicable.

- Where personal data is held on the premises, physical security forms part of the Company's reasonable security safeguards under the DPDP Act, 2023.

14. Incident Reporting and Breach Notification

- Any physical security incident (unauthorised access, break-in, lost/stolen credential or device, tailgating, missing records, environmental failure) must be reported immediately to **security@company.in** or **the Facilities Manager**.
- Incidents are logged, triaged and investigated; corrective and preventive actions are recorded.
- If a physical security incident involves a breach of personal data, the Company's data protection breach process is triggered, including notification to the Data Protection Board of India and affected data principals as required under the DPDP Act, 2023.
- If the incident is a reportable cyber security incident, it is reported to CERT-In within 6 hours of detection in line with the CERT-In Directions, 2022, coordinated by the **IT/Security Manager**.
- Where a criminal act (theft, break-in) has occurred, the Company may file a report with the local police.

15. Enforcement and Consequences

- Compliance with this policy is mandatory. Breaches may result in disciplinary action up to and including termination of employment or contract, in line with the Company's disciplinary process and the applicable Standing Orders or service rules.
- Contractors and vendors who breach this policy may have access revoked and engagements terminated.
- Deliberate circumvention of security controls, theft, or tampering may additionally lead to civil or criminal proceedings.
- Nothing in this policy reduces an employee's protections; reporting a security concern in good faith will not result in retaliation.

16. Review and Governance

This policy is owned by the **IT/Security Manager** and approved by **Management**. It is reviewed at least **annually**, or sooner on a significant change to premises, technology, organisational structure, an incident, or relevant law (including finalisation of the DPDP Rules, which remain evolving). The approved version, owner and effective date are recorded below.

Field	Value
Policy owner	**IT/Security Manager**
Approved by	**Management / Board**
Effective date	**DD-MMM-YYYY**
Version	**1.0**
Next review	**DD-MMM-YYYY**

[COMPANY NAME]

[Add your company logo / letterhead and registered address here]